Minimalizacja jednokierunkowego skończonego automatu kwantowego

mgr inż. Olga Siedlecka

olga.siedlecka@icis.pcz.pl

Instytut Informatyki Teoretycznej i Stosowanej
Politechnika Częstochowska

4 kwietnia 2008 roku



Plan wystąpienia

Wstęp

- Zastosowanie automatów
- Związek automatów niedeterministycznych, probabilistycznych i kwantowych
- Różnorodność definicji i typów automatów kwantowych
- Klasy języków akceptowanych przez automaty
- Minimalizacja automatów a relacja bisymulacji i relacja nierozróżnialności

Niedeterministyczny automat skończony

Definicja

Niedeterministycznym automatem skończonym - nazywamy piątkę $NFA = (Q, \Sigma, \delta, q_0, F)$, gdzie:

- Q - jest skończonym zbiorem stanów,
- Σ - jest alfabetem wejściowym,
- δ - jest funkcją przejść $\delta : Q \times \Sigma \mapsto 2^Q$,
- $q_0 \in Q$ - jest stanem początkowym,
- $F \subseteq Q$ - jest zbiorem stanów końcowych (akceptowalnych).

Jeżeli $NFA = (Q, \Sigma, \delta, q_0, F)$ jest niedeterministycznym automatem skończonym, to: $L(A) = \{w \in \Sigma^* : \hat{\delta}(q_0, w) \cap F \neq \emptyset\}$ jest językiem akceptowanym przez ten automat. Języki akceptowane przez niedeterministyczne automaty skończone nazywamy regularnymi [8].

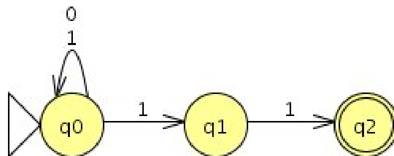
Przykład NFA

Przykład

Przykład niedeterministycznego automatu skończonego:
$NFA = (Q, \Sigma, \delta, q, F)$, gdzie:
$Q = \{q_0, q_1, q_2\}$ - jest skończonym zbiorem stanów,
$\Sigma = \{0, 1\}$ - jest alfabetem wejściowym,
$q = q_0$ - jest stanem początkowym,
$F = \{q_2\}$ - jest zbiorem stanów końcowych (akceptowalnych)

Funkcja przejść

$Q \setminus \Sigma$	0	1
q_0	$\{q_0\}$	$\{q_0, q_1\}$
q_1	$\emptyset$	$\{q_2\}$
q_2	$\emptyset$	$\emptyset$



Typy automatów probabilistycznych

- automaty reaktywne
- automaty generatywne
- automaty I\O
- automaty Vardi'ego
- automaty przemienne Hansson'a
- automaty Segala
- automaty łączone
- automaty Pnueli'ego-Zuck'a

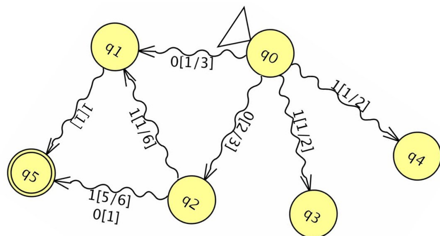
[12]

Reaktywny automat probabilistyczny

Definicja

Reaktywny automat probabilistyczny - to piątka $PA = (Q, \Sigma, \delta, q_0, F)$:

- Q - jest skończonym zbiorem stanów,
- Σ - jest alfabetem wejściowym,
- δ - jest funkcją prawdopodobieństwa przejść $\delta : Q \times \Sigma \mapsto \mathcal{D}(Q)$,
- $q_0 \in Q$ - jest stanem początkowym,
- $F \subseteq Q$ - jest zbiorem stanów końcowych (akceptowalnych).



Język akceptowany przez automat probabilistyczny

Notacja

Prawdopodobieństwo przejścia ze stanu q_1 do stanu q_2 po przeczytaniu symbolu σ zapisujemy jako $\delta(q_1, \sigma)(q_2) = p$. Rozszerzoną funkcję prawdopodbieństwa przejść zapisujemy:

$$\delta(q_1, w\sigma) = \sum_{q \in Q} \delta(q_1, w)(q) \cdot \delta(q, \sigma) \qquad [5]. \tag{1}$$

Definicja

Język akceptowany przez automat probabilistyczny to funkcja:

$$L_{PA} : \Sigma^* \mapsto (\frac{1}{2}, 1], \quad \text{taka że:} \quad \forall w \in \Sigma^*, L_{PA}(w) = \sum_{q \in F} \delta(q_0, w)(q) \quad [5]. \tag{2}$$

Odwracalny automat probabilistyczny

Definicja

Odwracalny automat probabilistyczny - to piątka $PRA = (Q, \Sigma, \delta, q_0, F)$

- Q - jest skończonym zbiorem stanów,
- Σ - jest alfabetem wejściowym,
- δ - jest funkcją prawdopodbieństwa przejść $\delta : Q \times \Sigma \mapsto \mathcal{D}(Q)$.
- $q_0 \in Q$ - jest stanem początkowym,
- $F \subseteq Q$ - jest zbiorem stanów końcowych (akceptowalnych).

Funkcja prawdopodbieństwa przejść spełnia następujące warunki:

$$\forall (q_1, \sigma_1) \in Q \times \Sigma \qquad \sum_{q \in Q} \delta(q_1, \sigma_1)(q) = 1 \tag{3}$$

$$\forall (q_1, \sigma_1) \in Q \times \Sigma \qquad \sum_{q \in Q} \delta(q, \sigma_1)(q_1) = 1 \qquad [6]. \tag{4}$$

Macierze podwójnie stochastyczne

Lemat

Dla każdego symbolu wejściowego $\sigma \in \Sigma$, funkcja prawdopodbieństwa przejść może być opisana przez macierz V_σ o rozmiarze $|Q|$ na $|Q|$, gdzie $(V_\sigma)_{i,j} = \delta(q_j, \sigma)(q_i)$. Wszystkie macierze V_σ są podwójnie stochastyczne jeżeli spełnione są warunki (3) i (4) [6].

Definicja

Macierz unitarna U jest prototypem dla podwójnie stochastycznej macierzy S jeżeli:

$$\forall i, j |U_{i,j}|^2 = S_{i,j} \qquad [6]. \tag{5}$$

Twierdzenie

Jeżeli wszystkie macierze odwracalnego automatu probabilistycznego maja unitarny prototyp, możemy go symulować za pomocą automatu kwantowego [6].

Typy automatów kwantowych:

- jednokierunkowy automat kwantowy [9]
- skończony automat kwantowy - jednokrotnej obserwacji [10]
- rozszerzony jednokierunkowy automat kwantowy [11]
- łotewski automat kwantowy [1]
- dwukierunkowy automat kwantowy [9]
- dwukierunkowy automat kwantowy ze stanami kwantowymi i klasycznymi [4]

Jednokierunkowy automat kwantowy

Definicja

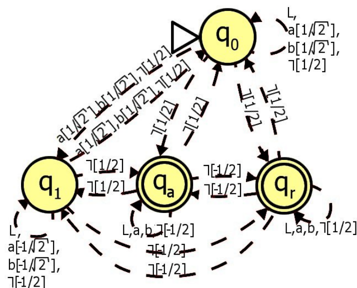
Jednokierunkowy automat kwantowy (definicja Kondacsa i Watrousa) to szóstka $1QFA = (Q, \Sigma, \delta, q_0, Q_a, Q_r)$, w której:

- Q - jest skończonym zbiorem stanów,
- Σ - jest alfabetem wejściowym,
- δ - jest funkcją przejść,
- $q_0 \in Q$ - jest stanem początkowym,
- $Q_a \subset Q$ - jest zbiorem stanów końcowych akceptujących,
- $Q_r \subset Q$ - jest zbiorem stanów końcowych odrzucających [9] [2].

Działanie 1QFA: I

Q_a i Q_r to zbiory stanów zatrzymujących; $Q_n = Q \setminus (Q_a \cup Q_r)$ - nie zatrzymujących. Symbole $\lfloor$ i $\rceil$ oznaczają lewy i prawy koniec słowa wejściowego, alfabet taśmy, na której operuje automat ma postać $\Gamma = \Sigma \cup \{\lfloor, \rceil\}$ [9] [2].

Funkcja przejść jest odwzorowaniem: $\delta : Q \times \Gamma \times Q \mapsto \mathbb{C}$.



Działanie 1QFA: II

Dla $\sigma \in \Gamma$, V_σ jest unitarnym operatorem na $l_2(Q)$ zdefiniowanym następująco:

$$V_\sigma(|q\rangle) = \sum_{q' \in Q} \delta(q, \sigma, q')|q'\rangle \qquad [9][2]. \tag{6}$$

W czasie obserwacji dokonywanych na automacie, wykorzystuje się obserwablę O odpowiadającą ortogonalnemu rozkładowi:

$$l_2(Q) = E_a \otimes E_r \otimes E_n, \tag{7}$$

gdzie $E_a = span\{|q\rangle | q \in Q_a\}$, $E_r = span\{|q\rangle | q \in Q_r\}$, $E_n = l_2(Q) - E_a - E_r$. Przez P_n oznacza się operator projekcji na podprzestrzeń E_n [7].

Skończony automat kwantowy

Definicja

Skończony automat kwantowy (definicja Moore'a i Crutchfielda) to piątka $QFA = (H, \Sigma, U_\sigma, |s_0\rangle, H_a)$, w której:

- H - jest skończoną przestrzenią Hilberta (przestrzenią stanów),
- Σ - jest alfabetem wejściowym,
- U_σ - są macierzami przejść dla każdego $\sigma \in \Sigma$,
- $|s_0\rangle \in H$ - jest stanem początkowym, spełniającym warunek $\langle s_0|s_0\rangle = 1$,
- $H_a \subset H$ - jest podprzestrzenią stanów akceptujących.

Zatem dla danego słowa w, automat będący w stanie początkowym $|s_0\rangle$, zostaje przekształcony poprzez zastosowanie unitarnej macierzy przejść: $U_w = U_{\sigma_0} U_{\sigma_1} \ldots U_{\sigma_n}$, po czym następuje obserwacja poprzez zastosowanie operatora rzutowania i wyliczenie normy [10].

Rozszerzony jednokierunkowy automat kwantowy

Definicja

Rozszerzony jednokierunkowy automat kwantowy - dla mieszanych stanów kwantowych (definicja Nayaka) to krotka $EQFA = (Q, \Sigma, U_\sigma, q_0, Q_a, Q_r)$, w której:

- Q - jest skończonym zbiorem stanów,
- Σ - jest alfabetem wejściowym,
- U_σ - są operatorami, będącymi złożeniem unitarnego przekształcenia i ortogonalnego pomiaru dla każdego $\sigma \in \Sigma$,
- $q_0 \in Q$ - jest stanem początkowym,
- $Q_a \subset Q$ - jest zbiorem stanów końcowych akceptujących,
- $Q_r \subset Q$ - jest zbiorem stanów końcowych odrzucających,
- $Q_n = Q \backslash \{Q_a \cup Q_c\}$ - jest zbiorem stanów niewstrzymujących [11].

Łotewski automat kwantowy

Definicja

Łotewski automat kwantowy - jednokierunkowy automat kwantowy, z jednokrotnym pomiarem, dla mieszanych stanów kwantowych (definicja Ambainisa i współautorów) to krotka $LQFA = (Q, \Sigma, A_\sigma, P_\sigma, q_0, Q_a)$, w której:

- Q - jest skończonym zbiorem stanów,
- Σ - jest alfabetem wejściowym,
- A_σ - są unitarnymi macierzami dla każdego $\sigma \in \Sigma$,
- P_σ - są pomiarami dla każdego $\sigma \in \Sigma$,
- $q_0 \in Q$ - jest stanem początkowym,
- $Q_a \subset Q$ - jest zbiorem stanów końcowych akceptujących,
- $Q_r = Q \backslash Q_a$ - jest zbiorem stanów odrzucających [1].

Twierdzenie

LQFA może symulować *PRA* jeżeli wszystkie jego macierze A_σ są unitarnymi prototypami macierzy stochastycznych. *PRA* może symulować *LQFA* jeżeli wszystkie pomiary P_σ zachowują $\oplus_{q \in Q} span\{|q\rangle\}$ dla każdego $\sigma \in \Sigma$ [1].

Dwukierunkowy automat kwantowy

Definicja

Dwukierunkowy automat kwantowy (definicja Kondacsa i Watrousa) to krotka $2QFA = (Q, \Sigma, \delta, D, q_0, Q_a, Q_r)$, w której:

- Q - jest skończonym zbiorem stanów,
- Σ - jest alfabetem wejściowym,
- δ - jest funkcją przejść,
- D - jest zbiorem symbolizującym kierunek przesunięcia głowicy odczytu na taśmie: $D = \{\leftarrow, \downarrow, \rightarrow\}$
- $q_0 \in Q$ - jest stanem początkowym,
- $Q_a \subset Q$ - jest zbiorem stanów końcowych akceptujących,
- $Q_r \subset Q$ - jest zbiorem stanów końcowych odrzucających [9] [7].

Dwukierunkowy automat kwantowy ze stanami kwantowymi i klasycznymi

Definicja

Dwukierunkowy automat kwantowy ze stanami kwantowymi i klasycznymi (definicja Ambainisa i Watrousa) to krotka $2QCFA = (Q, S, \Sigma, \Theta, \delta, D, q_0, s_0, S_a, S_r)$, w której:

- Q - jest skończonym zbiorem stanów kwantowych,
- S - jest skończonym zbiorem stanów klasycznych,
- Σ - jest alfabetem wejściowym,
- Θ - jest funkcją przejść w części kwantowej,
- δ - jest funkcją przejść w części klasycznej,

- D - jest zbiorem symbolizującym kierunek przesunięcia głowicy odczytu na taśmie: $D = \{\leftarrow, \downarrow, \rightarrow\}$
- $q_0 \in Q$ - jest początkowym stanem kwantowym,
- $s_0 \in S$ - jest początkowym stanem klasycznym,
- $S_a \subseteq S$ - jest zbiorem stanów końcowych akceptujących,
- $S_r \subseteq S$ - jest zbiorem stanów końcowych odrzucających [4].

Języki akceptowane przez automaty kwantowe

Definicja

Język kwantowy jest funkcją mapującą słowa na prawdopodobieństwa $L_Q : \Sigma^* \mapsto [0, 1]$ [10].

Twierdzenie

Język kwantowy rozpoznawany przez automat kwantowy zawiera słowa, które są akceptowane przez ten automat z prawdopodobieństwem większym niż $1/2$, zaś odrzucane z prawdopodobieństwem nie większym niż $1/2$ [9] [11].

Języki akceptowane przez automaty kwantowe

Twierdzenie

Wszystkie języki rozpoznawane przez automaty kwantowe są regularne. Istnieją języki regularne, które nie mogą być rozpoznane przez $1QFA$ z prawdopodbieństwem $1/2 + \epsilon$ dla każdego $\epsilon > 0$ [3].

Twierdzenie

Dwukierunkowy automat kwantowy rozpoznaje wszystkie języki regularne, a także niektóre nieregularne (np.: $L = \{a^i b^i | i \geqslant 1\}$) [9] [7].

Zestawienie automatów kwantowych

	C-automaty	DH-automaty
stany kwantowe czyste	*QFA*	1*QFA*, 2*QFA*
stany kwantowe mieszane	*LQFA*	*EQFA*
stany klasyczne i kwantowe czyste		2*QCFA*

Relacja równoważności

Definicja

Dla danego V_σ (równanie 6) zdefiniowane będzie v_σ równe odpowiednio: $v_\sigma[Q] = \sum_{q' \in Q} |\delta(q, \sigma, q')|^2$ (suma kwadratów wartości bezwzględnych amplitud) oraz $v_\sigma[S] = \sum_{q' \in S} |\delta(q, \sigma, q')|^2$ gdzie $S \subseteq Q$.

Lemat

Niech R będzie relacją równoważności na zbiorze S, A będzie zbiorem, zaś $V1, V2 \in l_2(S)$ będą unitarnymi operatorami odpowiadającymi przekształceniom układu kwantowego, zdefiniowanymi wzorem 6. Wówczas:

$$V1 \equiv_{R,A} V2 \iff \forall C \in S/R, \forall a \in A : v1_a[C] = v2_a[C]. \qquad (8)$$

Relacja bisymulacji

Definicja

Mając dwa skończone jednokierunkowe automaty kwantowe $1QFA_1 = (S, \Sigma, \delta)$ i $1QFA_2 = (T, \Sigma, \delta)$, można określić **relację silnej bisymulacji** $R \subseteq S \times T$, jeżeli dla wszystkich par $(s, t) \in R$ i dla wszystkich $\sigma \in \Sigma$ zachodzi:

- jeżeli $V1_\sigma(|s\rangle) = \sum_{s' \in S} \delta(s, \sigma, s')|s'\rangle$ wtedy istnieje $V2_\sigma(|t\rangle) = \sum_{t' \in T} \delta(t, \sigma, t')|t'\rangle$ takie, że $V1 \equiv_{R,\Sigma} V2$.

Relacja nierozróżnialności

Definicja

Mając dwa skończone jednokierunkowe automaty kwantowe $1QFA_1 = (S, \Sigma, \delta, s_0, S_a, S_r)$ i $1QFA_2 = (T, \Sigma, \delta, t_0, T_a, T_r)$, gdzie dodatkowo stany niewstrzymujące będą stanowić zbiory: $S_n = S \backslash (S_a \cup S_r)$ i $T_n = T \backslash (T_a \cup T_r)$, można określić **relację nierozróżnialności** $N \subseteq S \times T$, jeżeli dla wszystkich par $(s, t) \in N$ i dla wszystkich $\sigma \in \Sigma$ zachodzi:

- $(s, t) \in N^0$, wtedy i tylko wtedy, gdy $(s \in S_a \wedge t \in T_a) \vee (s \in S_r \wedge t \in T_r) \vee (s \in S_n \wedge t \in T_n)$,
- $(s, t) \in N^k$, wtedy i tylko wtedy, gdy $(s, t) \in N^{k-1}$ oraz
  - jeżeli $V1_\sigma(|s\rangle) = \sum_{s' \in S} \delta(s, \sigma, s')|s'\rangle$ wtedy istnieje $V2_\sigma(|t\rangle) = \sum_{t' \in T} \delta(t, \sigma, T')|t'\rangle$ takie, że $V1 \equiv_{R,\Sigma} V2$.

Automat ilorazowy

Twierdzenie

Relacja nierozróżnialności $\equiv$ jest kongruencją w zbiorze stanów automatu $1QFA = (Q, \Sigma, \delta, q_0, Q_a, Q_r)$ względem jego funkcji przejść δ.

Twierdzenie

Jeżeli relacja nierozróżnialności $\equiv$ na zbiorze stanów automatu $1QFA = (Q, \Sigma, \delta, q_0, Q_a, Q_r)$ względem jego funkcji przejść jest kongruencją, to istnieje automat ilorazowy $1QFA_{/\equiv} = (Q_{/\equiv}, \Sigma, \delta_{/\equiv}, [q_0]_\equiv, Q_{a/\equiv}, Q_{r/\equiv})$ (gdzie dla $\delta_{/\equiv}([q]_\equiv, \sigma)$ jest określone $V1_\sigma(|q\rangle)$, dla $[\delta(q, \sigma)]_\equiv$ jest określone $V2_\sigma(|q\rangle)$ i $V1 \equiv_{R,\Sigma} V2$), będący minimalnym automatem skończonym akceptującym ten sam język L_{1QFA}.

Minimalizacja 1QFA

Definicja

Automat skończony nazywa się minimalnym jeżeli wszystkie stany tego automatu są parami nierównoważne względem relacji nierozróżnialności.

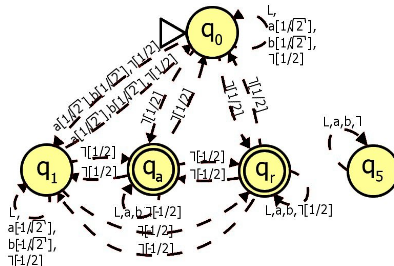
Twierdzenie

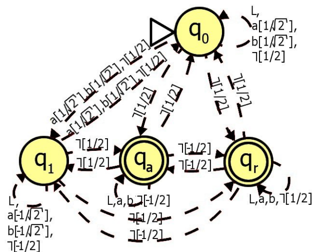
Automat A rozpoznający język L nazywa się **minimalnym**, gdy nie istnieje automat o mniejszej liczbie stanów rozpoznający L [8].

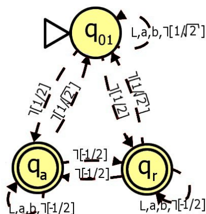
Metoda minimalizacji kwantowego automatu skończonego składa się z dwóch kroków:

- wyeliminowania stanów nieosiągalnych (po wyjściu ze stanu początkowego),
- złączenia stanów nierozróżnialnych.

Przykład minimalizacji 1QFA







Podsumowanie

- Teoria automatów kwantowych jako jeden z fundamentów teorii obliczeń kwantowych.
- Relacje bisymulacji i nierozróżnialności jako droga minimalizacji automatów kwantowych.
- Na bazie opisanej metody utworzono algorytm minimalizacji jednokierunkowego skończonego automatu kwantowego o złożoności $O(|\Sigma|n^3)$.


Ambainis, A., Beaudry, M., Golovkins, M., Kikusts, A., Mercer, M., and Thérien, D.
Algebraic results on quantum automata.
Theory of Computing Systems 39, 1 (2006), 165–188.


Ambainis, A., and Freivalds, R.
1-way quantum finite automata: strengths, weaknesses and generalizations.
In *FOCS '98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (Washington, DC, USA, 1998), IEEE Computer Society, pp. 332–341.


Ambainis, A., Kikusts, A., and Valdats, M.
On the class of languages recognizable by 1-way quantum finite automata.
In *STACS* (2001), vol. 2010 of *Lecture Notes in Computer Science*, Springer, pp. 75–86.


Ambainis, A., and Watrous, J.
Two-way finite automata with quantum and classical states.
Theoretical Computer Science 287 (2002), 299–311.


Cao, Y., Xia, L., and Ying, M.
Probabilistic automata for computing with words.
ArXiv Computer Science e-prints (2006).


Golovkins, M., and Kravtsev, M.
Probabilistic reversible automata and quantum automata.
Lecture Notes In Computer Science 2387 (2002), 574.


Gruska, J.
Quantum Computing.
McGraw-Hill, 1999.


Hopcroft, J. E., Motwani, R., and Ullman, J. D.
Introduction to Automata Theory, Languages, and Computation (2nd Edition).
Addison Wesley, 2000.


KONDACS, A., AND WATROUS, J.
On the power of quantum finite state automata.
In *IEEE, Symposium on Foundations of Computer Science* (1997), pp. 66–75.


MOORE, C., AND CRUTCHFIELD, J. P.
Quantum automata and quantum grammars.
Theoretical Computer Science 237, 1–2 (2000), 275–306.


NAYAK, A.
Optimal lower bounds for quantum automata and random access codes.
In *IEEE, Symposium on Foundations of Computer Science* (1999), pp. 369–377.


SOKOLOVA, A., AND DE VINK, E.
Probabilistic automata: System types, parallel composition and comparison.
In *Validation of Stochastic Systems: A Guide to Current Research* (2004), LNCS 2925, pp. 1–43.